ABSTRACT OF THE DISCLOSURE

A public-key cryptographic scheme of high efficiency capable of verifying security in a standard model. In order to retain security against adaptive chosen ciphertext attacks, a ciphertext is generated by a combination of a plaintext and random numbers so that an illegal ciphertext input to a (simulated) deciphering oracle is rejected.